(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
28 June 2001 (28.06.2001)

PCT

(10) International Publication Number
WO 01/47232 A2

(51) International Patent Classification[7]: H04M 7/00

(21) International Application Number: PCT/US00/35070

(22) International Filing Date:
22 December 2000 (22.12.2000)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/171,375 22 December 1999 (22.12.1999) US

(71) Applicant: TRANSNEXUS, INC. [US/US]; 1140 Hammond Drive, Building E, Suite 5250, Atlanta, GA 30328 (US).

(72) Inventors: THOMAS, Stephen; 4397 Windsor Oaks Circle, Marietta, GA 30066 (US). MCMANUS, Rodney, Scott; 1034 Briarhill Lane NE, Atlanta, GA 30324 (US). VAUGHN, Rick; 4383 Burnleigh Chase, Roswell, GA 30075 (US).

(74) Agents: WIGMORE, Steven, P. et al.; King & Spalding, 191 Peachtree Street, Atlanta, GA 30303 (US).

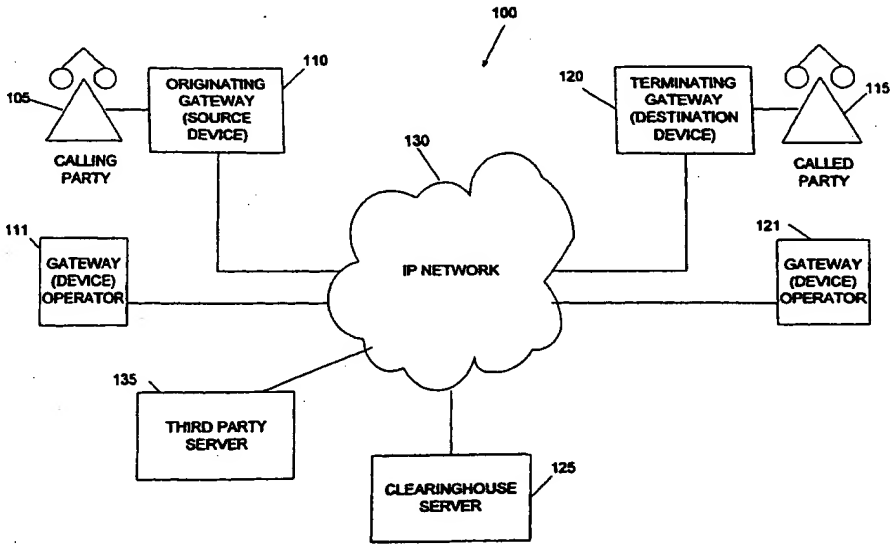
(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published:
— *Without international search report and to be republished upon receipt of that report.*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: SYSTEM AND METHOD FOR THE SECURE ENROLLMENT OF DEVICES WITH A CLEARINGHOUSE SERVER FOR INTERNET TELEPHONY AND MULTIMEDIA COMMUNICATIONS



(57) Abstract: Enrolling devices with a clearinghouse server for Internet telephony and multimedia communications. Enrollment can be the process of taking a network device (such as a router, gateway, gatekeeper, etc.) and exchanging encrypted information with the clearinghouse server, so that later communications with that device can be secured. The enrollment is done with levels of security and verification that ensures the devices and clearinghouse server is legitimate.

WO 01/47232 A2

SYSTEM AND METHOD FOR THE SECURE ENROLLMENT OF DEVICES WITH A CLEARINGHOUSE SERVER FOR INTERNET TELEPHONY AND MULTIMEDIA COMMUNICATIONS

Priority and Related Applications

The present application claims priority to provisional patent application entitled, "Automated Support of Internet Telephony Clearinghouse Services," filed on December 22, 1999 and assigned U.S. Application Serial Number 60/171,375. The present application is also related to the following pending applications: U.S. Provisional Patent Application Serial Number 60/231,642, entitled, "Clearinghouse Server for Internet Telephony and Multimedia Communications," filed on September 11, 2000, assigned to the assignee of the present application and hereby fully incorporated herein by reference; U.S. Application Serial Number, _____, entitled, "Call Detail Record Method and System for Internet Telephony Clearinghouse System," filed on December 22, 2000; U.S. Application Serial Number, _____, entitled, "User Interface for Internet Telephony Clearinghouse System," filed on December 22, 2000; and U.S. Application Serial Number, _____, entitled, "Rate Provisioning Method and System for Internet Telephony Clearinghouse System," filed on December 22, 2000.

TECHNICAL FIELD

The present invention is generally directed to telephony and multimedia communications carried by a distributed computer network, such as the global Internet. More specifically, the present invention relates to the secure enrollment of devices with a clearinghouse server so that communication can be routed between an originating device and a terminating device via the Internet.

BACKGROUND OF THE INVENTION

Telecommunications networks are experiencing a drastic technology shift--from a circuit-switched architecture (such as the current voice phone network) to a packet-switched architecture (such as the global Internet). Worldwide, the capacity of deployed packet-switched networks is doubling every year while circuit-switched capacity is only increasing at an annual rate of around 6%. In many developed regions, packet-switched capacity already exceeds circuit-

switched capacity. Recognizing this trend, telecommunications providers have begun to optimize their networks for the technology that is expected to dominate future growth: packet-switching. As they deploy packet-switched technology, these providers must still support traditional circuit-switched applications such as voice and facsimile. Instead of operating parallel network infrastructures, however, clearinghouse service providers seek to support those applications over a packet-switched network. This approach offers several advantages: greater efficiency through the use of a single, common, network infrastructure; lower cost through a reliance on packet-switching equipment; and better support of innovative new services through an open architecture.

As circuit-switched applications move to a packet-switched network, service providers need a way to identify systems on the packet-switched network that are associated with addresses (typically telephone numbers) common to the circuit-switched world. Providers must also have a means to authorize communications, and to ensure that unauthorized communications do not consume bandwidth. For example, the provisioning of a physical, circuit-switched, connection between two providers typically serves as authorization for the providers to share traffic. In a packet-switched environment, however, communicating parties need not share a physical connection and some other means of authorizing traffic is required. Finally, providers must have a reliable way to collect information from packet-switched devices to account for customer usage (e.g., for billing).

There remains a need in the art for a convenient, centralized application to provide authorization, or enrollment, for circuit-switched applications in a packet-switched network environment. Enrollment is the process of taking a device and exchanging sufficient cryptographic information with the clearinghouse server so that later communications with that device can be secured.

The conventional art does not provide an effective, secure way to enroll a device with a clearinghouse server. In particular, the identity of the clearinghouse server is verified by a telephone call. This verification has many drawbacks. Telephone calls are not automated, and require contact with people. As people have certain work hours, and cannot be relied upon to always be available, the telephone call verification is impractical, and time consuming. In addition, as packet-switched architecture becomes more and more popular, this problem will become more pronounced.

SUMMARY OF THE INVENTION

The present invention provides for the secure enrollment of a device for operation with a clearinghouse server, also described as a clearinghouse enrollment server, so that telephony and multimedia communications can be routed between an originating device and a terminating device via the Internet. The enrollment process is typically completed by a network device (such as a router, gateway, gatekeeper, etc.) and the clearinghouse server. This source device and the clearinghouse server can exchange encrypted information, so that later communications with that device can be secured. Once this verification process is finished, the device can have a public key certificate that is valid for a certain length of time (such as one year). Once this length of time has passed, however, the certificate can expire and the device must re-enroll. The enrollment process can also provide the device with a certificate authority's (CA) public key certificate. The device can use the CA's certificate to authenticate subsequent communications from other clearinghouse servers.

To enroll, the device can tell the clearinghouse server its public key. Then the device can prove that it possesses the private key that corresponds to the public key. This can be done by taking information provided by the clearinghouse enrollment server, and having the device encrypt it with the private key. The device can then send this information to the clearinghouse enrollment server. If the clearinghouse enrollment server can then decrypt the information, the clearinghouse enrollment server can verify that the device possesses the private key.

When the device tells the clearinghouse enrollment server its public key, a security issue arises. If an illegitimate user successfully intercepts, redirects, or captures the public key when it is sent to the clearinghouse enrollment server, the illegitimate user could take the place of the legitimate clearinghouse server. The illegitimate user could then be able to decrypt the encrypted message that the device sends, and would seem to be a legitimate clearinghouse enrollment server. Thus, the identity of the clearinghouse enrollment server must be verified.

Rather than using the conventional telephone call to verify the clearinghouse enrollment server's identity, the present invention can rely on the Web infrastructure to securely identify the clearinghouse enrollment server. The present invention does this by having the device pre-configured with a third party CA certificate. The clearinghouse enrollment server obtains a public key certificate under the authority of this CA certificate, and it provides that certificate, along with proof of possession of the corresponding private key, in the initial communications with the device.

In view of the foregoing, it will be appreciated that the present invention provides a method for secure enrollment of a device with services of a clearinghouse enrollment server to supporting communications carried by an Internet telephony system. A device can initiate a request to enroll for the services of the clearinghouse enrollment server. In turn, the identity of the clearinghouse enrollment server is verified a communication exchange between the device and the clearinghouse enrollment server. This exchange is supported by use of a security infrastructure comprising the Secure Sockets Layer (SSL) and a public key infrastructure. In response to verifying the identity of the clearinghouse enrollment server, enrollment of the device is completed at the clearinghouse enrollment server to all the device to access the communication services of the Internet telephony network.

More specifically, the present invention provides a for secure enrollment of a device with services of a clearinghouse server for an Internet telephony system. In response to obtaining an identity of the clearinghouse server, the device issues a CA certificate request to the clearinghouse server using that obtained identity. In response to the CA certificate request, the clearinghouse server transmits a CA certificate to the device. The device next determines whether the clearinghouse is a valid and secure service provider by verifying the CA certificate. Responsive to verification of the CA certificate, the device generates a combination of a private key and a public key and issues to the clearinghouse server a request for enrollment comprising the public key. In turn, the clearinghouse server generates a public key certificate and transmits the public key certificate to the device. This enables the device to securely verify the identity of the clearinghouse server and to complete device enrollment at the clearinghouse server.

These and other aspects of the present invention will be shown in the attached drawing set and following detailed description.

BRIEF DESCRIPTION OF THE DRAWINGS

Fig. 1 is a functional block diagram of the operating environment in accordance with an exemplary embodiment of the present invention.

Fig. 2 is a functional block diagram of the architecture of a clearinghouse server in accordance with an exemplary embodiment of the present invention.

Fig. 3A is a logical flow chart diagram illustrating steps for enrolling a source device for operation with a clearinghouse server in accordance with an exemplary embodiment of the present invention.

Fig. 3B is a logical flow chart diagram illustrating steps for completing an enrollment request by a source device in accordance with an exemplary embodiment of the present invention.

DETAILED DESCRIPTION OF THE EXEMPLARY EMBODIMENTS

The present invention provides a clearinghouse solution for routing multi-media communications, including telephony calls, between a source device and a destination device via a distributed computer network, such as the global Internet. The present invention also authorizes the completion of a communication from a source device to a destination device and collects usage-related information for the completed communication. The clearinghouse server constructed in accordance with the inventive concept can identify one or more available destination devices available to accept a communication from an authorized source device based upon the source of that communication. An exemplary embodiment of the clearinghouse server can operate in either a "WINDOWS" or "SOLARIS" operating system environment in support of Web-based communications in a distributed computer network.

Turning now to the drawings, in which like reference numbers identify like elements of exemplary embodiments of the present invention, Fig. 1 is a functional block diagram illustrating a representative operating environment for an exemplary embodiment of the present invention. A communication system 100 comprises one or more originating devices (such as gateways) 110, one or more terminating devices (such as gateways) 120, device operators 111 and 121 for each of the two devices, a clearinghouse server 125, and a third party server 135, each coupled to an Internet Protocol (IP) network 130. Although Fig. 1 illustrates an operating environment including only a single originating gateway 110 and a single terminating gateway 120, those skilled in the art will appreciate that the operating environment of the communication system 100 can include multiple originating gateways and terminating gateways. For purposes of this document, an originating gateway will be referred to as a source device, and a terminating gateway will be referred to as a terminating device. The IP network 130 represents a distributing computer network and can be implemented by the global Internet, a wide area network (WAN), or an enterprise-wide local area network (LAN).

To initiate a communication supported by the communication system 100, a calling party 105 sends an outgoing call having a called telephone number to the source device 110. For this representative example, the calling party 105 has an established a relationship with the source device 110, such as a subscription to call origination services provided by that source device. To be an authorized user of the clearinghouse services provided by the clearinghouse server 125, the gateway operators 111 or 121 can enroll source device 110 and destination device 120 for operation with the clearinghouse server 125. The enrollment process involves the exchange of information between the gateway operators 111 or 121, the clearinghouse server 125, and the third party server 125. (not affiliated with either the operators or clearinghouse server). This enrollment process is the subject of the present invention. Following the enrollment process, the source device 110 sends an authorization request message to the clearinghouse server 125 via the IP network 130 to request the completion of the outgoing call with an available designation device 120. The authorization request typically comprises the called telephone number, otherwise described as the dialed number, a call identifier to uniquely identify the outgoing call and, for certain applications, the telephone number for the calling party 105 and payment authorization, such as a calling card number and a personal identification number (PIN).

If the clearinghouse server 125 determines that the source device 110 is an authorized user of clearinghouse services, the clearinghouse server 125 can identify one or more destination devices for handling the outgoing call. The source device 110 can use the information provided by the clearinghouse server 125 in the authorization response to contact a selected destination device 120 and to complete the incoming call via the IP network 130. In turn, the selected destination device 120 can communicate the outgoing call to a called party 115, typically via the Public Switched Telephone Network (PSTN). In this manner, the outgoing call is connected between the calling party 105 and the called party 115 by a combination of a distributed computer network and the PSTN.

Fig. 2 is a functional block diagram illustrating the components of a clearinghouse server constructed in accordance with an exemplary embodiment of the present invention. An exemplary clearinghouse server 125 comprises an operating system 205, a Web server 210, an XML parser, a clearinghouse engine 220, and a user interface 225. The clearinghouse server 125 can be coupled to a database comprising one or more configuration files 230 to support clearinghouse operations.

The platform of the clearinghouse server 125 is provided by the operating system 205, which is preferably implemented by Microsoft Corporation's "WINDOWS 2000" or Sun Microsystem's "SOLARIS" operating systems. Although the "WINDOWS" and the "UNIX" platforms represent preferred platforms, it will be appreciated that the inventive concept of a clearinghouse server 125 can be supported by other operating systems and is not limited to those described herein. The operating system 205 communicates with the Web server 210.

The Web server 210 supports Web-based communications with client computers in a Web-enabled computing environment, including the source devices illustrated in Fig. 1. The XML parser 215 can accept messages from the clearinghouse engine 220 and convert those messages to XML format for communication via the Web server 210. The XML parser 215 also can extract information from an XML message received by the Web server 210 and supply the extracted information to the clearinghouse engine 220. The Web server 210 also communicates with the user interface 225 via application programming interfaces (APIs). The Web server 210 is preferably implemented by an "XITAMI" server available from iMatix Corporation sprl of Antwerpen, Belgium.

The clearinghouse engine 220 supports the processing of clearinghouse transactions and communicates with the operating system 205, the Web server 210, and the user interface 225. APIs can be used to access functions supported by the clearinghouse engine 220. The clearinghouse engine 220 also can access configuration files maintained by the configuration database 230 in support of clearinghouse transactions. The configuration files typically contain descriptive information identifying characteristics of enrolled source devices and clearinghouse transaction records, including transaction identifiers assigned to transactions by the clearinghouse server 125.

The user interface 225 provides a mechanism for a user, such as an assistant administrator, to input information about the clearinghouse environment, including details about enrolled source devices and destination devices. The user interface 225 also can present the user with information related to clearinghouse transaction records stored by the clearinghouse server 125.

Secure Enrollment

Referring again to Figure 1, the present invention provides a system and method for the secure enrollment of a device for operation with a clearinghouse server 125. Enrollment is the process of taking a network device

(such as a router, gateway, gatekeeper, etc.) and exchanging encrypted information with the clearinghouse server 125, so that later communications with that device can be secured. There are several types of devices, including originating devices 110 and terminating devices 120. As the process of enrollment is described, all devices will be referred to as originating or source devices 110. This is not meant to limit the applicable devices to only source devices, but is meant to illustrate that any type of device can be used. Once this process is finished, the device 110 should have a certificate that is valid for a certain length of time (such as one year). Once this length of time has passed, the certificate will expire and the device 110 must re-enroll.

This invention works for any type of service or device 110 that requires secured communications. This includes devices 110 under the direct control of human users (like a personal computer or a IP-based telephone) and those that are automated and not under the direct control of human users.

Exemplary Encryption Environment

In light of the discussion of public keys and private keys, a general discussion of an exemplary encryption environment may prove beneficial for understanding the present invention. Encryption is the process of encoding data to prevent unauthorized access, especially during transmission. Encryption is usually based on one or more keys, or codes, that are essential for decoding, or returning the data to readable form. An encryption key is a sequence of data that is used to encrypt other data and that, consequently, must be used for the data's decryption. Decryption is the process of restoring encrypted data to its original form.

Public key encryption is a process that uses a pair of keys for encryption: a private (secret) key and a public key. The private key can encrypt messages and can create a unique electronic number (called a digital signature) that can be read by anyone possessing the corresponding public key. The private key can also be used to decrypt messages encrypted with the public key. The public key can be used for encrypting messages to be sent to the user and for decrypting the user's digital signature.

A certification authority ("CA") is an organization that assigns digital certificates. A CA may be an external issuing company (such as VeriSign) or an internal company authority that has installed its own certificate server 125 (such as a Microsoft Certificate Server) for issuing and verifying certificates. A CA is responsible for verifying the identity of a party and, if that identity is accepted, digitally signing that party's public key certificate. Other parties (that

possess and trust the CA's public key, can then verify the applicant's identity merely by verifying the CA's signature of the public key certificate.

A CA certificate (sometimes called a digital certificate) is a user identity card for cyberspace. Issued by a CA, a CA certificate is an electronic credential that demonstrates that a user or site is trusted for the purpose of security and computer authentication.

Overview of Exemplary Enrollment Process

The enrollment process begins when the device generates a public/private key pair. It then establishes a secure communication channel with the clearinghouse enrollment server using the Secure Sockets Layer (SSL) protocol. The SSL exchange provides the device with a public key certificate for the enrollment server. That certificate is digitally signed by the third party certificate authority, who, therefore, vouchsafes for the enrollment server's identity.

Once the secure communications path is established, the enrollment server sends the device CA certificates of a (potentially different) certificate authority. Certificates certified by this additional CA will be used in subsequent communications with the clearinghouse. The additional CA may be the same CA as is authenticating the enrollment server, but it need not be so. By permitting them to differ, the present invention allows for different public key infrastructures for enrollment and for operational clearinghouse communications (e.g. routing telephone calls).

After receiving the CA certificate, the device then sends the enrollment server the previously generated public key. The enrollment server receives this public key and, either immediately or at a later time (e.g. after an administrator has verified that the customer intended to enroll the device in question), the enrollment server issues the device a certificate containing the device's public key.

Message Formats

All messages sent to the clearinghouse enrollment server are carried in HTTP (version 1.1) POST messages. All replies are returned in responses to the POST. Each POST request contains a series of ASCII variable=value pairs, encoded as given in RFC 1738. Any response also consists of variable/value pairs. The following Table 1 lists the variables that can be included in a message. Note

that non-alphanumeric characters are encoded as a "%" and their corresponding two hexadecimal digits (as specified in RFC 1738.)

Table 1

cacert=<cert>	base64-encoded authority certificate
certreq=<pkcs10>	base64-encoded certificate request
customer=<custID>	clearinghouse-assigned customer number
device=<devID>	clearinghouse-assigned device id
nonce=<nonce>	random value to increase security
operation=<req. type>	getcacert, request, or retrieve
password=<pwd>	password for clearinghouse services
username=<username>	username for clearinghouse services

The following example in Table 2 shows a sample CA certificate request message. In it, the device asks for the enrollment server's CA certificate in cleartext:

Table 2

```
POST  HTTP/1.1
Host: enroll.transnexus.com
content-type: text/plain
Content-Length: 19
Connection: Keep-Alive

operation=getcacert
```

The response received from the enrollment server might look like the example shown in Table 3:

Table 3

```
HTTP/1.1 200 OK
Server: TNS/1.0
Connection: Keep-Alive
Content-Type: text/plain
Content-Length: 693

status=0&certificate=MIIB9DCCAV2gAwIBAgIRANs4gtN4kbWXlwvw8YsAjxMwD
QYJKoZIhvcNAQEEBQAwFTETMBEGA1UEChMKVHJhbnNOZXh1czAeFw05OTAzMTgwMDA
wMDBaFw0wOTAzMTgyMzU5NTlaMBUxEzARBgNVBAoTClRyYW5zTmV4dXMwgZ8wDQYJK
oZIhvcNAQEBBQADgY0AMIGJAoGBAKuR4hI8P+g96Go7ihjfdQ+3VjA01pIqNjaSch+
eWWzbBG+q+aISa0sQM53elNuxMudoCFN27J7H4v0LuStDj+wSQzWjP41BOQUXry1tR
```

i+qwRaK5VhlwybHejOByURb4Qex5myhEbNWAxOimgCBIB2Exf4k5FJjOMUs795rlUp
XAgMBAAGjRDBCMCIGA1UdEQQbMBmkFzAVMRMwEQYDVQQDEwpPbnNpdGUyLTYyMA8GA
1UdEwQIMAYBAf8CAQAwCwYDVR0PBAQDAgEGMA0GCSqGSIb3DQEBBAUAA4GBAEgeTxN
56ztf2bzu2Zx1a/e0IWexTeEbjCQNNEZaFOLhp50kVB6oQQkX726Oiv0Gx4IJdTv3Y
HYc7BOi1pU0jWlPc/DVkhHdlQ/gDSNFgwAqJCx2nml-fr9TuEtAUWAxd/PN38//yDyX
Wgx5PKyU9+pyLPgCoAC8D17wMGdh+oTSm

Once the CA certificate is retrieved, the certificate request is encrypted and transmitted to the enrollment server for approval. The initial request (before it is encrypted) looks like the representative example shown in Table 4:

Table 4

```
POST  HTTP/1.1
Host: enroll.transnexus.com
content-type: text/html
Content-Length: 714
Connection: Keep-Alive

operation=request&nonce=1502767911902931&username=mcmanus&password
=01234567&device=134217728&customer=0&request=MIIBtTCCAR4CAQAwWzEL
MAkGA1UEBhMCVVMxEDAOBgNVBAgTB0dlb3JnaWExGDAWBgNVBAoTD1RyYW5zTmV4dX
MsIExMQzEgMB4GA1UEAxMXdGVzdHRlcDQudHJhbnNuZXh1cy5jb20wgZ8wDQYJKoZI
hvcNAQEBBQADgY0AMIGJAoGBALhYeWbF8HrVIRVMW4p2H2DZhs9tEisHe1ynyUEIcC
4n9CLW104HW0zeSzNMtYBQrqJ6qZMhc0RKZ%2BMQA9E1S9hvN8TLo4KDBPXmQWEQg6
R9f3TokpIhOJ4bOwpj9WeXAiyNyTq7hTgQdtPYN65xq92t5CkHpWBWEya9v2Ux9I27
AgMBAAGgGjAYBgkqhkiG9w0BCQcxCxMJcGFzc3dvcmQAMA0GCSqGSIb3DQEBBAUAA4
GBAFC7sCjCbmVgUYenJR8XgMtLilQFSSq4YJ9BcmiYsZZ6KOxFxNgEf84wyRscdrP9
LV9EhQM%2BS3gEAEw%2FLxCRHGGgyS1%2FYpNmavs51thGeplH%2BAFW%2Blnds9CY
UwyKx%2F8veFJFC6y6pYhD7RyZxyKNnzBhgxAxU3rUgr3Cm78RbT1G
```

The retrieve function only differs in the "operation" parameter, in which the "request" value is replaced by "retrieve". Otherwise, all parameters have the same names and values.

If the enrollment request is pending further approval, then the enrollment server is only required to send the status of the certificate request. It may send a nonce along with the response, but this value is not guaranteed. The response should look like the representative example shown in Table 5:

Table 5

```
HTTP/1.1 200 OK
content-type: text/plain
content-length: 31

status=1&nonce=A1F0765F71C9E6AD
```

If the enrollment request has been processed and accepted by the server, it will return a response such as the following in Table 6. Note that a status of 0 indicates that the certificate is now ready for retrieval.

Table 6

```
HTTP/1.1 200 OK
content-type: text/plain
content-length: 694

status=0&cert=MIICfjCCAeegAwIBAgIQARAm+prL9zmocfkRWNN0fjANkqhkiG9w
0BAQQFADAV...
```

Fig. 3A is a logical flow chart diagram illustrating exemplary steps completed during the enrollment of a source device for operation with a clearinghouse server. Turning now to Fig. 3A, an exemplary enrollment process 300 is initiated in response to a user, typically an assistant administrator, defining a source device to be enrolled as a "user" or subscriber of clearinghouse services. A source device is typically identified by an IP address or a Domain Name System (DNS) name. In addition, the administrator can assign the source device to a particular Group of devices having one or more common characteristics.

In step 310, commands are issued at the source device to complete an enrollment request for transmission to the clearinghouse server. These commands are typically device dependent and often require support by an administrator to select the appropriate enrollment instructions. Representative enrollment request tasks completed by the source device for step 310 are shown in the logical flow chart diagram of Fig. 3B.

Turning briefly to Fig. 3B, the source device obtains the identity of the clearinghouse server in step 330. The identity is typically an IP address or a DNS name for the clearinghouse server. In step 335, the source device obtains a certificate authority (CA) certificate from the clearinghouse server 335 based upon an initial contact with the identified clearinghouse server via the IP network. In

decision step 340, an inquiry is conducted to determine if the CA certificate can be verified as a certificate issued by a trusted device. For example, the verification task in decision step 340 can be completed by an administrator of the source device contacting a representative of the services offered by the clearinghouse server to verify the CA certificate. If the CA certificate can not be verified in decision step 340, the "NO" branch is followed to step 345 and the enrollment request process is terminated at the source device. Based on a positive response, however, the "YES" branch is followed from decision step 340 to step 350. In step 350, the source device generates a public/private key pair and sends an enrollment request with the public key to the clearinghouse server 350 via the IP network. Upon device enrollment, a configuration record or file for that device is constructed for storage in the configuration database accessible by the clearinghouse server.

Returning now to Fig. 3A, the source device sends an enrollment request via the IP network to the clearinghouse server in step 315. Responsive to the enrollment request, the clearinghouse server creates a public key certificate and sends that certificate to the source device via the IP network. This public key can be used by the source device to initiate secure communications with the clearinghouse server. In step 325, the clearinghouse server obtains device information and builds a configuration file for the source device. The configuration file is maintained at the configuration database and is accessible by the clearinghouse server. A representative configuration file is shown in Table 7.

Table 7

```
license 'software license key'
crypto 'keys'
enroll enabled
routing enabled
cdrs enabled
ssl enabled
group ''
group 'ACME ITSP'
group 'BT-Concert'
group 'HK Telecom'
group 'Prepaid'
device 'device8.isp.com' '' enabled enrolled
device 'device1.itsp.com' 'ACME ITSP' enabled enrolled
device 'device2.itsp.com' 'ACME ITSP' enabled enrolled
device 'device3.itsp.com' 'ACME ITSP' disabled enrolled
```

```
device 'device4.carrier.com' 'BT-Concert' enabled enrolled
device 'device4.com' 'HK Telecom' enabled
device 'device5.com' 'HK Telecom' disabled
device 'device6.isp.com' 'Prepaid' enabled enrolled
device 'device7.isp.com' 'Prepaid' enabled enrolled
route " '+1...' 'device1.itsp.com' 60 'device2.itsp.com' 25 'device3.itsp.com' 15
    'device4.carrier.com' 0
route " '+1 404...' 'device1.itsp.com' 75 'device2.itsp.com' 25 'device4.carrier.com' 0
route " '+1 770...' 'device1.itsp.com' 75 'device2.itsp.com' 25 'device4.carrier.com' 0
route " '+33...' 'device4.com' 1 'device5.com' 0
route " '+33 6...' 'device4.com' 1 'device5.com' 0
route " '+46...' 'device4.com' 1 'device5.com' 0
route " '+46 70...' 'device4.com' 1 'device5.com' 0
route " " 'device6.isp.com' 100 'device7.isp.com' 0 'device8.isp.com' 0
route 'ACME ITSP' '+1...' 'device1.itsp.com' 60 'device2.itsp.com' 25
    'device3.itsp.com' 15 'device4.carrier.com' 0
route 'ACME ITSP' '+1 404...' 'device1.itsp.com' 75 'device2.itsp.com' 25
    'device4.carrier.com' 0
route 'ACME ITSP' '+1 770...' 'device1.itsp.com' 75 'device2.itsp.com' 25
    'device4.carrier.com' 0
route 'ACME ITSP' '+33...' 'device4.com' 1 'device5.com' 0
route 'ACME ITSP' '+33 6...' 'device4.com' 1 'device5.com' 0
route 'ACME ITSP' '+46...' 'device4.com' 1 'device5.com' 0
route 'ACME ITSP' '+46 70...' 'device4.com' 1 'device5.com' 0
route 'ACME ITSP' " 'device6.isp.com' 100 'device7.isp.com' 0 'device8.isp.com' 0
route 'BT-Concert' '+1...' 'device1.itsp.com' 60 'device2.itsp.com' 25
    'device3.itsp.com' 15 'device4.carrier.com' 0
route 'BT-Concert' '+1 404...' 'device1.itsp.com' 75 'device2.itsp.com' 25
    'device4.carrier.com' 0
route 'BT-Concert' '+1 770...' 'device1.itsp.com' 75 'device2.itsp.com' 25
    'device4.carrier.com' 0
route 'BT-Concert' '+33...' 'device4.com' 1 'device5.com' 0
route 'BT-Concert' '+33 6...' 'device4.com' 1 'device5.com' 0
route 'BT-Concert' '+46...' 'device4.com' 1 'device5.com' 0
route 'BT-Concert' '+46 70...' 'device4.com' 1 'device5.com' 0
route 'BT-Concert' " 'device6.isp.com' 100 'device7.isp.com' 0 'device8.isp.com' 0
```

```
route 'HK Telecom' '+1...' 'device1.itsp.com' 60 'device2.itsp.com' 25
    'device3.itsp.com' 15 'device4.carrier.com' 0
route 'HK Telecom' '+1 404...' 'device1.itsp.com' 75 'device2.itsp.com' 25
    'device4.carrier.com' 0
route 'HK Telecom' '+1 770...' 'device1.itsp.com' 75 'device2.itsp.com' 25
    'device4.carrier.com' 0
route 'HK Telecom' '+33...' 'device4.com' 1 'device5.com' 0
route 'HK Telecom' '+33 6...' 'device4.com' 1 'device5.com' 0
route 'HK Telecom' '+46...' 'device4.com' 1 'device5.com' 0
route 'HK Telecom' '+46 70...' 'device4.com' 1 'device5.com' 0
route 'HK Telecom' " 'device6.isp.com' 100 'device7.isp.com' 0 'device8.isp.com' 0
route 'Prepaid' " 'device1.itsp.com' 60 'device2.itsp.com' 25 'device3.itsp.com' 15
    'device4.carrier.com' 0
```

Each line in a configuration file (other than comments or blank lines) contains a single configuration item. The first word on the line identifies that item. The possible values for this word are listed below in Table 8.

Table 8

license:	software license key for the clearinghouse server
crypto:	cryptographic keys for the clearinghouse server
enroll:	flag to enable/disable device enrollment
routing:	flag to enable/disable call routing
cdrs:	flag to enable/disable CDR collection
ssl:	flag to force clearinghouse server requests to use SSL for security
group:	a group (convenient collection) of devices
device:	a device (gateway, gatekeeper, proxy, softswitch, etc.)
route:	a route for a call

The same configuration item may be included multiple times in this file. In such cases, the clearinghouse server's behavior depends on the specific item. In most cases, later occurrences of an item will override an earlier value. For example, if multiple "license" lines are included in the file, only the last line will actually be used by the server. In the case of "group", "device", and "route", multiple occurrences define additional groups, devices, or routes. Note, however,

that it is not possible to define multiple groups with the same name, multiple devices with the same name, or multiple routes with the same group and called number. If the configuration file attempts to define duplicates, the server will generate an error when attempting to read and parse the file.

license "software license key"

The content following the license keyword should be a software license key enclosed in double quotation marks. If this parameter is absent from the file, or if the included license key is invalid, the underlying software supporting operations of the clearinghouse server will revert to a trial version. New software license keys may be obtained from a licensor of the clearinghouse server software. They can either be added to the configuration file manually or imported into the server through the user interface. Imported license keys are stored in configuration backups. Unlike other configuration items, old values of the license key are kept in the configuration file, allowing a straightforward reversion to an earlier license (by deleting the newest license keys), as well as problem diagnosis and auditing.

crypto "cryptographic parameters"

The content following the crypto keyword should be cryptographic parameters for the clearinghouse server enclosed in double quotation marks. If this parameter is absent, the clearinghouse server will automatically generate new cryptographic parameters. If this occurs, though, all enrolled devices will have to re-enroll with the server to refresh their cryptographic knowledge.

enroll {enabled | disabled}

The content following the enroll keyword should be a single word, either "enabled" or "disabled" (without the quotation marks), whichever is appropriate. If this parameter is not present, device enrollment will be disabled.

routing {enabled | disabled}

The content following the routing keyword should be a single word, either "enabled" or "disabled" (without the quotation marks), whichever is appropriate. If this parameter is not present, call routing will be disabled.

cdrs {enabled | disabled}

The content following the call details records) (cdrs) keyword should be a single word, either "enabled" or "disabled" (without the quotation

marks), whichever is appropriate. If this parameter is not present, CDR collection will be disabled.

ssl {enabled | disabled}

The content following the ssl keyword should be a single word, either "enabled" or "disabled" (without the quotation marks), whichever is appropriate.

group name

The content following the group keyword should be the name of the group. If the name consists of more than one word, the entire name should be enclosed in double quotation marks.

device name group {enabled | disabled} [enrolled]

The content following the device keyword should be the DNS name of the device, the name of the group to which the device belongs (enclosed in quotation marks if the name is more than one word), the word "enabled" or "disabled" (without the quotation marks), and, optionally, the word "enrolled" (also without quotation marks).

route group number (device weight)

The content following the route keyword should be the name of the group to which the route applies (enclosed in quotation marks if the name is more than one word), the called number prefix for the routes (enclosed in quotation marks if the number includes spaces) and then a series of one or more device weight pairs, where device is the DNS name of the destination device, and weight is the weighting factor for that device.

It should be understood that the foregoing relates only to illustrative embodiments of the present invention, and numerous changes may be made therein without departing from the spirit and scope of the invention as defined by the following claims.

What is claimed is:

1. A method for secure enrollment of a device with services of a clearinghouse enrollment server supporting communications completed by an Internet telephony system, comprising the steps:

initiating a request by the device to enroll for the services of the clearinghouse enrollment server;

verifying an identity of the clearinghouse enrollment server by using a security infrastructure comprising the Secure Sockets Layer (SSL) and a public key infrastructure; and

responsive to verifying the identity of the clearinghouse enrollment server, completing enrollment of the device to access the services of the clearinghouse enrollment server.

2. A method for secure enrollment of a device with services of a clearinghouse server for an Internet telephony system, comprising the steps:

obtaining an identity of the clearinghouse server;

issuing a CA certificate request from the device to the clearinghouse server using the obtained identity;

responsive to the CA certificate request, transmitting a CA certificate from the clearinghouse server to the device;

determining by the device the verification of the CA certificate;

responsive to verification of the CA certificate, generating a combination of a private key and a public key and issuing to the clearinghouse server a request from the device for enrollment comprising the public key;

responsive to the device enrollment request, generating a public key certificate at the clearinghouse server and transmitting the public key certificate to the device, thereby enabling the device to securely verify the identity of the clearinghouse server; and

responsive to verifying the identity of the clearinghouse server, completing enrollment of the device to access the services of the clearinghouse server.

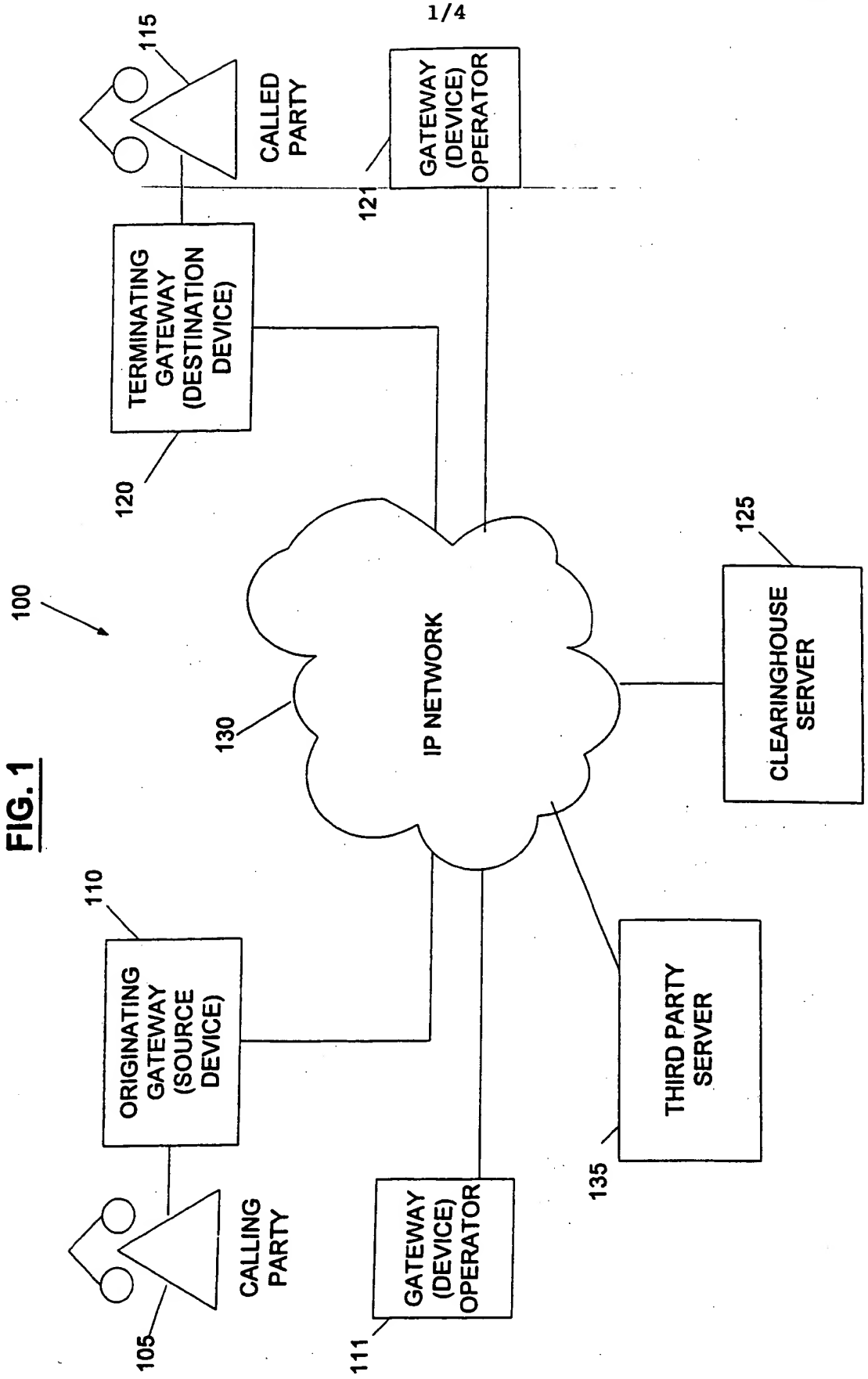

100
IP NETWORK
130
CLEARINGHOUSE SERVER
125
THIRD PARTY SERVER
135
ORIGINATING GATEWAY (SOURCE DEVICE)
110
CALLING PARTY
105
GATEWAY (DEVICE) OPERATOR
111
TERMINATING GATEWAY (DESTINATION DEVICE)
120
CALLED PARTY
115
GATEWAY (DEVICE) OPERATOR
121

FIG. 1

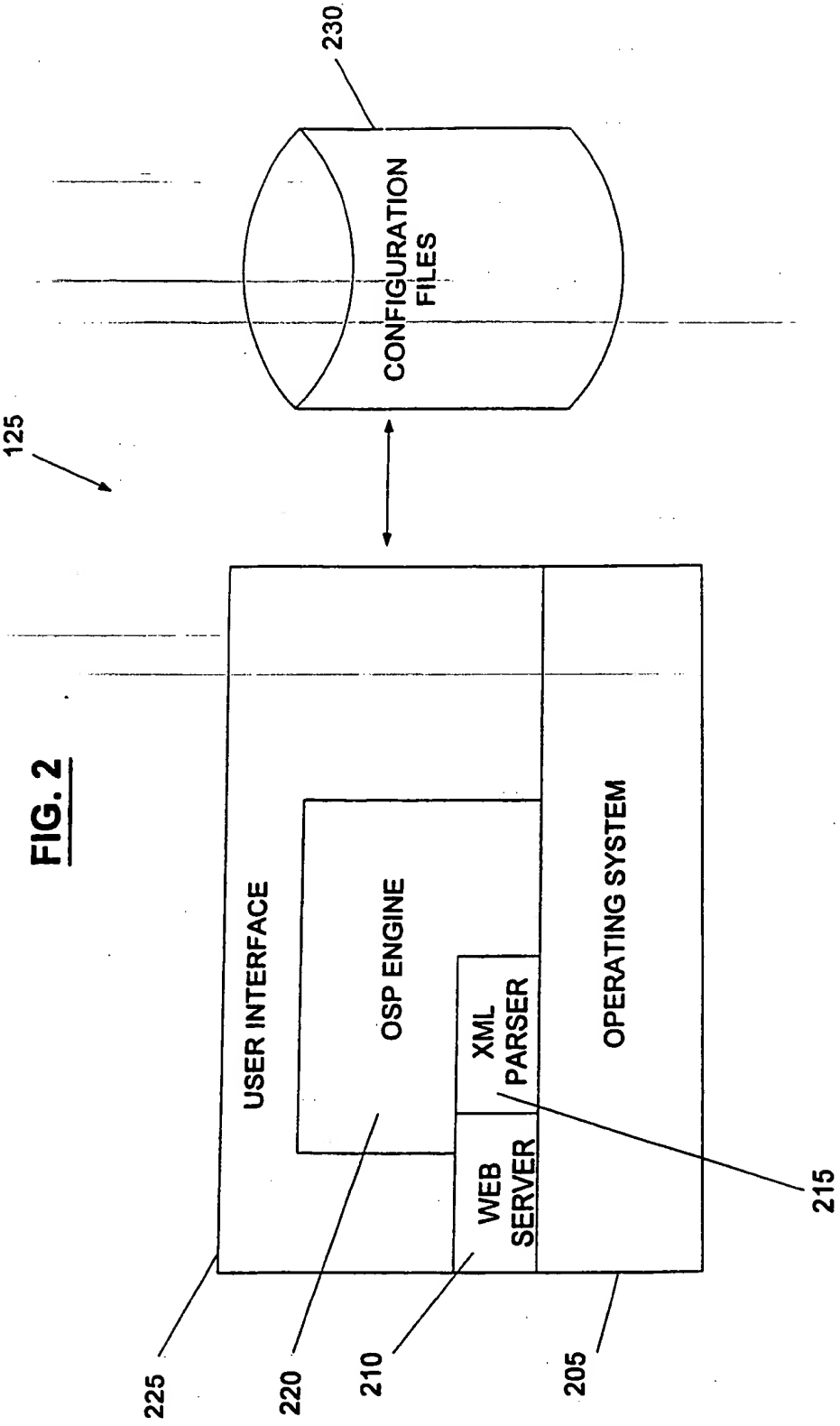

230
CONFIGURATION FILES
125
USER INTERFACE
OSP ENGINE
XML PARSER
WEB SERVER
OPERATING SYSTEM
225
220
210
205
215

FIG. 2

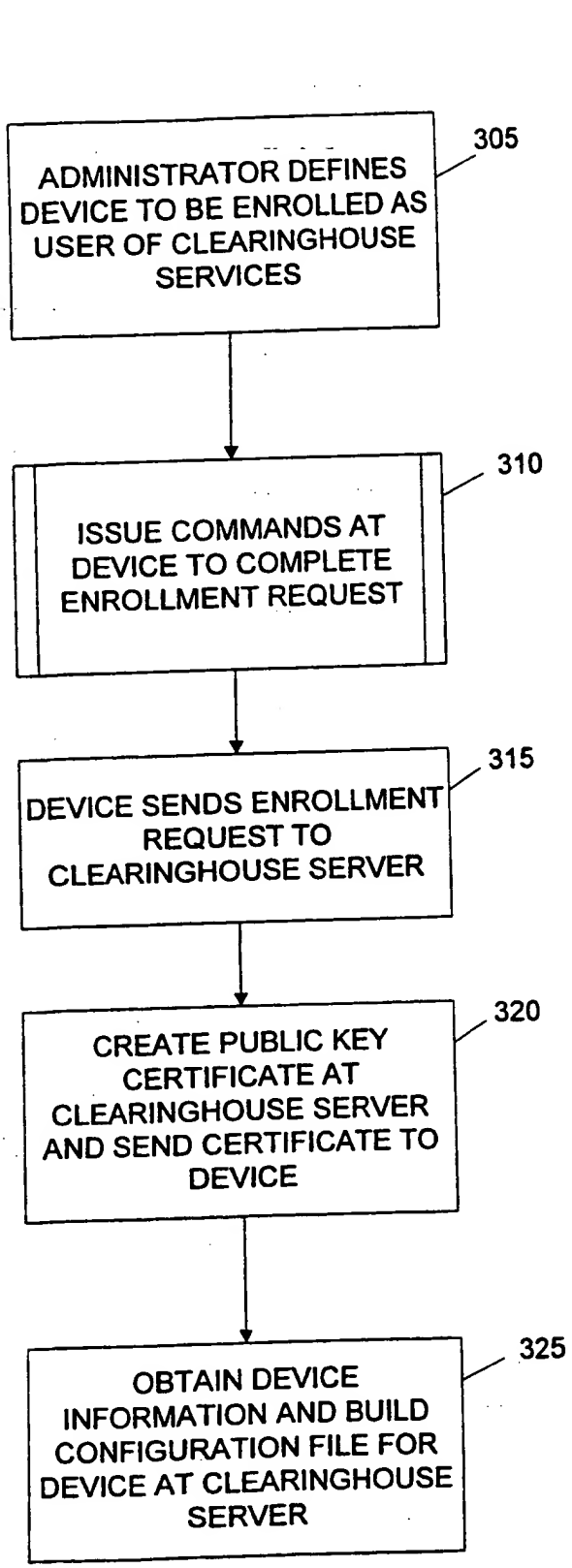

300
ADMINISTRATOR DEFINES DEVICE TO BE ENROLLED AS USER OF CLEARINGHOUSE SERVICES
305
ISSUE COMMANDS AT DEVICE TO COMPLETE ENROLLMENT REQUEST
310
DEVICE SENDS ENROLLMENT REQUEST TO CLEARINGHOUSE SERVER
315
CREATE PUBLIC KEY CERTIFICATE AT CLEARINGHOUSE SERVER AND SEND CERTIFICATE TO DEVICE
320
OBTAIN DEVICE INFORMATION AND BUILD CONFIGURATION FILE FOR DEVICE AT CLEARINGHOUSE SERVER
325

Fig. 3A

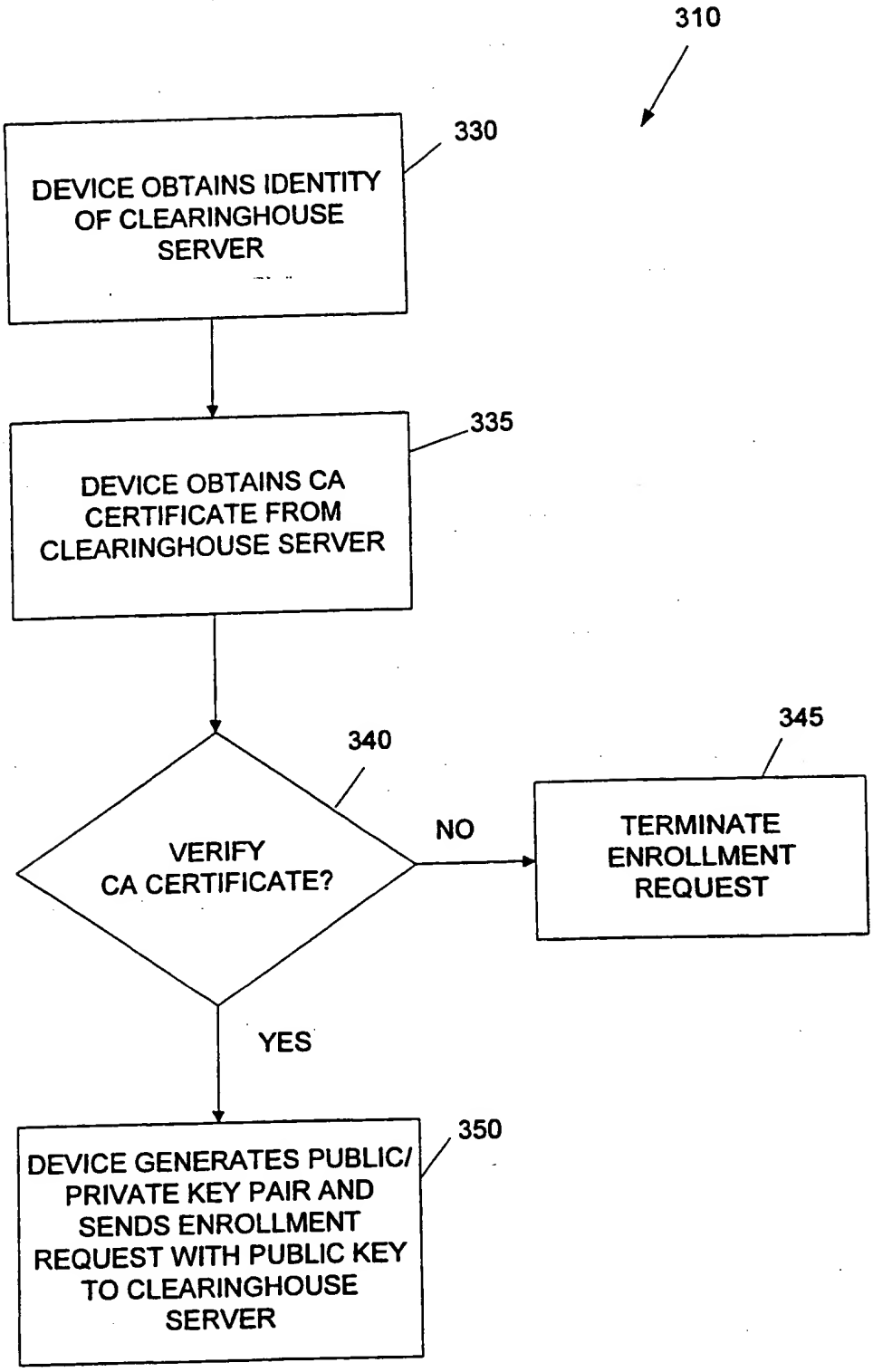

310
DEVICE OBTAINS IDENTITY OF CLEARINGHOUSE SERVER
330
DEVICE OBTAINS CA CERTIFICATE FROM CLEARINGHOUSE SERVER
335
VERIFY CA CERTIFICATE?
340
NO
TERMINATE ENROLLMENT REQUEST
345
YES
DEVICE GENERATES PUBLIC/ PRIVATE KEY PAIR AND SENDS ENROLLMENT REQUEST WITH PUBLIC KEY TO CLEARINGHOUSE SERVER
350

Fig. 3B